FIPS 140-2 Level 3
Non-Proprietary Security Policy
NITROXIII CNN35XX-NFBE HSM Family

Document Number: CNN35xx-NFBE-SPD-L3
Document Version: Version 1.2
Revision Date: 7/6/2022

Revision History

Revision	Date	Author	Description of Change
1.0	9/20/2021	Rajendar Kalwa	Entropy updates and ACVP certs updates for transition algorithms
1.1	6/7/2022	Rajendar Kalwa	Addressed review comments from NIST Updated build number with Diagnostics enhancement
1.2	7/6/2022	Rajendar Kalwa	Section 7.1 updated to explicitly state the minEntropy value per 8-bit output.

Table of Contents

List of Tables

List of Figures

1 Module Overview

The Marvell (formerly Cavium Inc.) NITROXIII CNN35XX-NFBE HSM Family (hereafter referred to as *the module or HSM*) is a high-performance purpose-built security solution for crypto acceleration. The module provides a FIPS 140-2 overall Level 3 security solution. The module is deployed in a PCIe slot to provide crypto and TLS 1.0/1.1/1.2 acceleration in a secure manner to the system host. It is typically deployed in a server or an appliance to provide crypto offload. The module's functions are accessed over the PCIe interface via an API defined by the module.

The module is a hardware/firmware multi-chip embedded cryptographic module. The module provides cryptographic primitives to accelerate approved and allowed algorithms for TLS 1.0/1.1/1.2 and SSH. The cryptographic functionality includes modular exponentiation, random number generation, and hash processing, along with protocol specific complex instructions to support TLS 1.0/1.1/1.2 security protocols using the embedded NITROXIII chip. The module implements password based single factor authentication at FIPS 140-2 Level 3 security. The physical boundary of the module is the outer perimeter of the card itself.

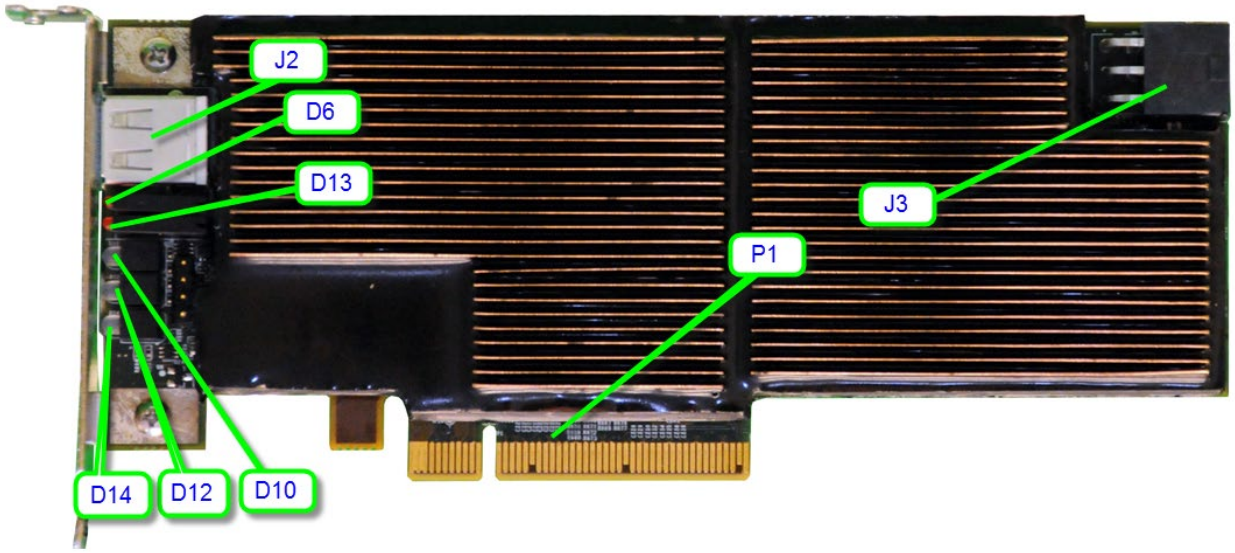

Figure 1 – Top View of Cryptographic Module

Table 1 – LED Description

LED Location	LED Description
D6 – Red	Power Fail indication
D6 – Green	Power OK – All voltages rails are at nominal
D13 – Red	See Table 7
D13 – Green	See Table 7
D10 –Multicolor	See Table 7
D12 - Multicolor	See Table 7
D14 - Multicolor	See Table 7

The configuration of hardware and firmware for this validation is:

Table 2 – Hardware Part Numbers

Part Number	LiquidSecurity Appliance	Cores Enabled	Key Store Size	Max Partitions
CNL3560P-NFBE-G	Yes	64	100K	32
CNL3560P-NFBE-2.0-G	Yes	64	100K	32
CNL3560P-NFBE-3.0-G	Yes	64	100K	32
CNL3560B-NFBE-2.0-G	Yes	64	100K	32
CNL3560B-NFBE-3.0-G	Yes	64	100K	32
CNL3560-NFBE-G	Yes	64	100K	32
CNL3560-NFBE-2.0-G	Yes	64	100K	32
CNL3560-NFBE-3.0-G	Yes	64	100K	32
CNL3560A-NFBE-3.0-G	Yes	64	100K	32
CNL3560C-NFBE-3.0-G	Yes	64	100K	32
CNL3560D-NFBE-3.0-G	Yes	64	100K	32
CNL3560E-NFBE-3.0-G	Yes	64	100K	32
CNL3560F-NFBE-3.0-G	Yes	64	100K	32
CNL3530-NFBE-G	Yes	32	25K	32
CNL3530-NFBE-2.0-G	Yes	32	25K	32
CNL3530-NFBE-3.0-G	Yes	32	25K	32
CNL3530B-NFBE-2.0-G	Yes	32	25K	32
CNL3530B-NFBE-3.0-G	Yes	32	25K	32
CNL3530A-NFBE-3.0-G	Yes	32	25K	32
CNL3530C-NFBE-3.0-G	Yes	32	25K	32
CNL3530D-NFBE-3.0-G	Yes	32	25K	32
CNL3530E-NFBE-3.0-G	Yes	32	25K	32
CNL3530F-NFBE-3.0-G	Yes	32	25K	32
CNL3510-NFBE-G	Yes	24	25K	24
CNL3510-NFBE-2.0-G	Yes	24	25K	24
CNL3510-NFBE-3.0-G	Yes	24	25K	24
CNL3510P-NFBE-G	Yes	32	50K	32
CNL3510P-NFBE-2.0-G	Yes	32	50K	32
CNL3510P-NFBE-3.0-G	Yes	32	50K	32
CNL3510A-NFBE-3.0-G	Yes	32	50K	32
CNL3510C-NFBE-3.0-G	Yes	32	50K	32
CNL3510D-NFBE-3.0-G	Yes	32	50K	32
CNL3510E-NFBE-3.0-G	Yes	32	50K	32
CNL3510F-NFBE-3.0-G	Yes	32	50K	32
CNN3560P-NFBE-G	No	64	100K	64
CNN3560P-NFBE-2.0-G	No	64	100K	64
CNN3560P-NFBE-3.0-G	No	64	100K	64
CNN3560-NFBE-G	No	64	50K	32
CNN3560-NFBE-2.0-G	No	64	50K	32
CNN3560-NFBE-3.0-G	No	64	50K	32
CNN3560A-NFBE-3.0-G	No	64	50K	32
CNN3560C-NFBE-3.0-G	No	64	50K	32
CNN3560D-NFBE-3.0-G	No	64	50K	32
CNN3560E-NFBE-3.0-G	No	64	50K	32
CNN3560F-NFBE-3.0-G	No	64	50K	32
CNN3530-NFBE-G	No	32	25K	32
CNN3530-NFBE-2.0-G	No	32	25K	32
CNN3530-NFBE-3.0-G	No	32	25K	32

CNN3530A-NFBE-3.0-G	No	32	25K	32
CNN3530C-NFBE-3.0-G	No	32	25K	32
CNN3530D-NFBE-3.0-G	No	32	25K	32
CNN3530E-NFBE-3.0-G	No	32	25K	32
CNN3530F-NFBE-3.0-G	No	32	25K	32
CNN3510-NFBE-G	No	24	25K	24
CNN3510-NFBE-2.0-G	No	24	25K	24
CNN3510-NFBE-3.0-G	No	24	25K	24
CNN3510A-NFBE-3.0-G	No	24	25K	24
CNN3510C-NFBE-3.0-G	No	24	25K	24
CNN3510D-NFBE-3.0-G	No	24	25K	24
CNN3510E-NFBE-3.0-G	No	24	25K	24
CNN3510F-NFBE-3.0-G	No	24	25K	24
CNN3510LP-NFBE-2.0-G	No	24	25K	24
CNN3510LP-NFBE-3.0-G	No	24	25K	24
CNN3510LPB-NFBE-2.0-G	No	24	25K	24
CNN3510LPB-NFBE-3.0-G	No	24	25K	24
CNN3510LPA-NFBE-3.0-G	No	24	25K	24
CNN3510LPC-NFBE-3.0-G	No	24	25K	24
CNN3510LPD-NFBE-3.0-G	No	24	25K	24
CNN3510LPE-NFBE-3.0-G	No	24	25K	24
CNN3510LPF-NFBE-3.0-G	No	24	25K	24
CNN3505LP-NFBE-2.0-G	No	16	10K	16
CNN3505LP-NFBE-3.0-G	No	16	10K	16
CNN3505LPA-NFBE-3.0-G	No	16	10K	16
CNN3505LPC-NFBE-3.0-G	No	16	10K	16
CNN3505LPD-NFBE-3.0-G	No	16	10K	16
CNN3505LPE-NFBE-3.0-G	No	16	10K	16
CNN3505LPF-NFBE-3.0-G	No	16	10K	16

LP is low-frequency part, where N3 chip runs at 500MHz, otherwise it runs at 600MHz.

CNN3510-NFBE-G Firmware:

CNN35XX-NFBE-FW-1.1 build 02 and CNN35XX-NFBE-FW-1.1 build 05

The module supports different performance options as listed above in the hardware identifier. The physical hardware and firmware are identical across all options. The underlying hardware has multiple identical cryptographic engines which are enabled or disabled using an option parameter set at manufacturing time. Also, Manufacturer can configure the HSM adapter to work only with Cavium's Marvell's LiquidSecurity HSM appliances, these parts are identified with CNL prefix. CNN cards can work with non-Marvell (Cavium) appliances.

The major blocks of the module are: General purpose MIPS based control processor, crypto processors, RAM memory, NOR and eMMC flash for persistent storage, USB interfaces, and PCIe gen-2 x8 interfaces.

2 Security Level

The cryptographic module meets the overall requirements applicable to Level 3 security of FIPS 140-2.

Table 3 – Module Security Level Specification

Security Requirements Section	Level
Cryptographic Module Specification	3
Module Ports and Interfaces	3
Roles, Services and Authentication	3
Finite State Model	3
Physical Security	3
Operational Environment	N/A
Cryptographic Key Management	3
EMI/EMC	3
Power on Self-Tests	3
Design Assurance	3
Mitigation of Other Attacks	N/A

3 Modes of Operation

The module supports the following modes of operation:

1) Non-FIPS mode of operation
2) FIPS Approved Level 3 mode of operation

The module is initialized into one of the modes specified above during the module initialization period. The value of the parameter fipsState passed into the call specifies the mode. The following are the allowed values for fipsState parameters:

0 - Non-FIPS mode

2 - FIPS Approved mode with single factor authentication mechanism

3 - FIPS Approved mode with certificate based dual factor authentication mechanism

The indicator of Approved mode is obtained by using the Get Status service. The fipsState field of Get Status service indicates the mode.

3.1 FIPS Approved Mode of Operation

The module provides a FIPS Approved mode of operation, comprising all services described in Section 6.3 below. In this mode, the module allows only FIPS Approved or allowed algorithms. Request for any non-Approved/allowed algorithm is rejected.

3.2 Non-FIPS Mode of Operation

The Module supports a Non-FIPS mode implementing the non-FIPS Approved algorithms listed in Table 6.

3.3 Partitions

N3FIPS adapter is a sr-iov enabled intelligent PCIe adapter with 1 physical function and 128 virtual functions. In addition to the crypto offloads, this adapter can provide secure key storage with up to 64 partitions, including master partition. Each partition will have its own users to manage the partition and own configuration policies and hence each partition can be treated as a virtual HSM. HSM always has one default partition called HSM Master partition and this contains configuration of the complete HSM and default configuration of any additional partitions that are created. Only one HSM partition can be assigned to one sr-iov virtual function of HSM adapter and vice-versa. Keys belonging to one partition are not accessible from another partition, this is achieved through a secure binding between partition and the PCIe virtual function.

3.3.1 HSM Master Partition

This is the default partition with only one user, called the Master Crypto Officer (MCO). This partition represents the operating state of the whole HSM adapter. I.e. initialization of HSM is nothing but initializing this partition with required configuration and MCO credentials. Zeroizing this partition will erase all HSM partitions in the adapter. The HSM has to be initialized and the MCO should already be logged in to create more partitions on the adapter. The MCO can backup and restore complete partition including user data, partition configuration and user keys. All the backup data is encrypted with Backup keys.

3.3.2 HSM Partition

Each partition will have a different set of users to manage it and a dedicated key storage and crypto resources associated. A partition will have a default configuration supplied by the master partition and can be changed (within limits) during the partition initialization. When a partition is created by the MCO, it will be in zeroized state and has to be initialized to do any keystore management or crypto function offloads. Partition initialization will create the Partition Crypto Officer (PCO). The PCO can later create up to 6 Partition Crypto Users (PCUs) on demand. Each user will have a unique username to identify the users. The User has to login to the partition/vHSM to issue any authorized commands. Users are authenticated using passwords submitted during the user creation.

4 Supported Cryptographic Algorithms

This section provides the list of supported cryptographic algorithms segregated based on the operating mode.

4.1 Approved and Allowed Algorithms

The cryptographic module supports the following FIPS Approved algorithms.

Table 4 – FIPS Approved Algorithms Used in the Module

FIPS Approved Algorithm	Usage	Certificate
AES: – ECB mode: Encrypt/Decrypt; 128, 192 and 256-bit – CTR mode: 128, 192 and 256-bit	Data encryption and decryption	2033
AES: – ECB mode: Encrypt/Decrypt; 128, 192 and 256-bit – CBC mode: Encrypt/Decrypt; 128, 192 and 256-bit	Data encryption and decryption	2034
AES: – GCM: Encrypt/Decrypt; 128, 192 and 256-bit – 96-bit random IV; TLS record encryption – GMAC is supported – IG A.5 Notes: – TLS 1.2 or other applications can offload GCM operations. – For TLS-1.2 protocol, IV constructed as described in RFC 5288. – IV is generated internally to the cryptographic module. – IV is not generated internally to the GCM algorithm boundary. – SP 800-38D §8.2.2 is used for GCM IV construction. – IVs are generated randomly, and IG A.5 Requirement #2 applies. – IV's free field is a 4-byte counter. – IV's random field is a 96-bit random number. – IV's random field is incremented by 1. IV's random field wouldn't overflow 96-bits in the lifetime of the module. – Internal Approved RNG: SP 800-90A DRBG, AES_CTR 256-bit. – Internal NDRNG used to seed the Approved RNG: Octeon HW random number generator	Data encryption and decryption	2035
AES: – ECB mode: Encrypt/Decrypt; 128, 192 and 256-bit – CTR mode: 256-bit	DRBG and Keywrap	3205
AES: – SP 800-38F AES Key Wrap, AES 256-bit	Key backup/restore	3206 (AES)

FIPS Approved Algorithm	Usage	Certificate
CKG – IG D.12 – SP 800-133 Section 6.1 Asymmetric signature key generation using unmodified DRBG output – SP 800-133 Section 6.2 Asymmetric key establishment key generation using unmodified DRBG output – SP 800-133 Section 7.1 Direct symmetric key generation using unmodified DRBG output – SP 800-133 Section 7.3 Derivation of symmetric keys from a key agreement shared secret. – SP 800-133 Section 7.4 Derivation of symmetric keys from a pre-shared key	Key Generation	Vendor Affirmed
CVL - SP 800-56A ECC CDH: P-224 and P-256 with SHA-256, P-384 and P-521 with SHA-512	ECDH compute and SSL suite B key exchange	563 (CVL)
CVL - SP 800-56B RSADP – Modulus Length: 2048-bit	RSA decryption	A1936 (CVL), A1937 (CVL)
CVL - TLS-KDF ((v1.0/1.1, v1.2))	TLS handshake	167 (CVL)
DRBG SP 800-90A: AES-CTR 256-bit	Key generation	680
DSA: – PQG Gen: 2048 and 3072-bit (SHA-256) – PQG Ver: 1024-bit (SHA-1); 2048 and 3072-bit (SHA-256) – Key Gen: 2048 and 3072-bit – Sig Gen: 2048-bit (SHA-224, -256, -384, -512) – SigVer: 1024, 2048 and 3072-bit (SHA-1, 224, -256, -384, -512)	Key generation, Sign, Verify	916
ECDSA: – PKG: P-224, P-256, P-384, P-521, K-233, K-283, K-409, K-571, B-233, B-283, B-409, and B-571 – PKV: All P, K and B curves – Sig Gen: P-224, P-256, P-384, P-521, K-233, K-283, K-409, K-571, B-233, B-283, B-409, and B-571 (SHA-224, -256, -384, -512) – SigVer: All P, K and B curves (SHA-1, 224, -256, -384, -512)	Key generation, Sign and Verify	589
ENT SP800-90B	System entropy	N/A
HMAC: SHA-1, 224, 256, 384 and 512	MAC generation	1233
HMAC-SHA-1,224, 256, 384, 512	MAC generation and KAS	2019
KAS: – KAS-ECC SP800-56Ar3 – Ephemeral Unified with no Key confirmation with – P-521 with SHA-512	Cloning	A1934
KAS-RSA: – SP 800-56B RSA/IFC based KAS using 2048-bit key size 3072 and 4096-bit key size tested, but not used.	Key agreement	A1935
KBKDF SP 800-108 HMAC-SHA-256 KDF	KBK generation	65 (KBKDF)

FIPS Approved Algorithm	Usage	Certificate
KTS – AES KW	Key transport	3206
RSA: – KeyGen: 2048 and 3072-bit – PKCS #1 1.5 SigGen: 2048 and 3072-bit (SHA-224, -256, -384, -512) – PKCS #1 1.5 SigVer: 1024, 2048 and 3072-bit (SHA-1, 224, -256, -384, -512)	Key generation, Sign, Verify	1634
RSA: – KeyGen: 4096-bit – PKCS #1 1.5 SigGen: 4096-bit (SHA-224, -256, -384, -512) – PKCS #1 1.5 SigVer: 4096 (SHA-1, 224, -256, -384, -512) PKCS PSS SigGen and SigVer tested, but not used.	Key generation, Sign, Verify	A1936
SHA: 1, 224, 256, 384, and 512	Data hashing	1780
SHA: 1, 224, 256, 384, and 512	Signature generation, verification, HMAC. SHA-1 in only verify.	2652
Triple-DES: – TECB mode; 3-key – TCBC mode; 3-key	Data encryption and decryption Module limits Triple-DES encryptions to 2^16 64-bit blocks per IG A.13.	1311

The cryptographic module supports the following non-FIPS Approved algorithms which are allowed for use in FIPS mode.

Table 5 – FIPS Allowed Algorithms Used in the Module

Algorithm	Usage
MD5 (no security claimed)	Hashing within TLS
RSA (CVL Cert #A1936, key wrapping; key establishment methodology provides between 112 and 150 bits of encryption strength)	Key Wrapping (Octeon) KBK unwrap

The support of TLS 1.0/1.1/1.2 protocol by the module is restricted to the TLS Key Derivation Function and the crypto operation. This functionality of the module is used by the user of the module as part of TLS protocol negotiation. The TLS protocol has not been reviewed or tested by the CAVP or CMVP.

4.2 Non-Approved, Non-Allowed Algorithms

The cryptographic module supports the following non-Approved algorithms available only in non-FIPS mode.

Table 6 – Non-Approved, Non-Allowed Algorithms Used in the Module

Algorithm	Usage	Keys/CSPs
PBE	Key generation	Password
RC4	Encryption/Decryption	RC4 key of 128 bits

4.3 LED Error Pattern for FIPS Failure

On successful completion of the FIPS tests, the LED remains in the "ON" state. Blinking indicates failures on the HSM. If the LED remains in the permanent glow, the card's state is fine. All blinks are 200ms ON and 200ms OFF. Blink delay time gap is 1000ms.

Table 7 – LED Flash Pattern for Errors

FIPS Test	LED Pattern					
	LED No.	Color	Red	Green	Blue	Blinks
N3 AES-CBC Encrypt/Decrypt	D12	Red	Y	N	N	1
N3 AES-ECB Encrypt/Decrypt	D12	Blue	N	N	Y	1
N3 AES-GCM Encrypt/Decrypt	D12	Blue	N	N	Y	6
N3 Triple-DES-CBC Encrypt/Decrypt	D12	Red	Y	N	N	2
N3 SHA	D12	Red	Y	N	N	3
N3 HMAC	D12	Blue	N	N	Y	2
N3 KDF	D12	Blue	N	N	Y	7
N3 RSA Enc and Dec	D12	Blue	N	N	Y	8
Octeon AES ECB Encrypt/Decrypt	D12	Green	N	Y	N	9
Octeon DRBG	D12	Green	N	Y	N	4
Octeon RSA Sign/Verify	D12	Red	Y	N	N	4
Octeon/N3 Key Gen	D12	Red	Y	N	N	5
Octeon DSA Sign Gen/Verify	D12	Red	Y	N	N	7
Octeon PQG Gen/Verify	D12	Red	Y	N	N	8
Octeon ECDSA Sig/Verify	D12	Green	N	Y	N	7
Octeon ECDSA PKV	D12	Green	N	Y	N	6
Octeon SHA	D12	Green	N	Y	N	2
Octeon HMAC	D12	Green	N	Y	N	3
Octeon KAS	D12	Green	N	Y	N	8
Octeon AES Key Wrap	D12	Blue	N	N	Y	10
ECDSA pair wise consistency test	D12	Blue	N	N	Y	4
RSA pair wise consistency test	D12	Blue	N	N	Y	5
DSA pair wise consistency test	D12	Green	N	Y	N	1
ECDH Test	D12	Red	Y	N	N	10
Octeon KDF	D12	Red	Y	N	N	11
Octeon RSA Enc and Dec	D12	Red	Y	N	N	6
ENT Health tests	D12	Red	Y	N	N	9
Firmware Power-on Tests						
Nitrox device file creation	D14	Red	Y	N	N	1
Nitrox driver load fails	D14	Red	Y	N	N	2

FIPS Test	LED Pattern					
	LED No.	Color	Red	Green	Blue	Blinks
Nitrox micro code load fails	D14	Red	Y	N	N	3
Nitrox pot test failures	D14	Red	Y	N	N	4
Database creation fails	D14	Red	Y	N	N	5
Mgmt daemon has not started successfully	D14	Red	Y	N	N	6
HW RNG for firmware	D12	Blue	N	N	Y	3
Other Firmware States						
HSM Boot stage 1	D10	Red	Y	N	N	No blink
HSM Boot stage 2	D10	Red	Y	N	N	Blink (definite)
HSM Boot stage 3(SE-APP initialized Linux handshake not done)	D10	Violet	Y	N	N	No blink
HSM Linux handshake done, host driver handshake not done	D10	Violet	Y	N	N	Infinite
HSM PF driver handshake complete	D10	Blue	Y	N	N	Infinite
HSM admin driver handshake done	D10	Green		Y	N	No blink
FS recovery: - All fine	D13		N	N	NA	Does not flash anything
FS recovery: - Log partn corrupted	D13	Green	N	Y	NA	No blink
FS recovery: - main partn corrupted	D13	Red	Y	N	NA	No blink
FS recovery: - more than 1 partn corrupted/recovery fails	D13		Y	Y	NA	No blink
FS recovery: NAND flash corrupted	D13		Y	Y	NA	Blink

4.4 TLS 1.0/1.1/1.2 Cipher Suites

The module supports the following cipher suites using FIPS Approved and allowed algorithms and key sizes:

- TLS_RSA_AES256-GCM-SHA384
- TLS_RSA_AES128-GCM-SHA256
- TLS_RSA_AES256-SHA256
- TLS_RSA_AES256-SHA
- TLS_RSA_DES-CBC3-SHA
- TLS_RSA_AES128-SHA256
- TLS_RSA_AES128-SHA
- TLS_ECDH_RSA_ AES_128_CBC_SHA256
- TLS_ECDH_RSA_ AES_256_CBC_SHA384
- TLS_ECDH_RSA_ AES_128_GCM_SHA256
- TLS_ECDH_RSA_ AES_256_GCM_SHA384
- TLS_ECDH_ECDSA_ AES_128_CBC_SHA256
- TLS_ECDH_ECDSA_ AES_256_CBC_SHA384

- TLS_ECDH_ECDSA_ AES_128_GCM_SHA256
- TLS_ECDH_ECDSA_ AES_256_GCM_SHA384
- TLS_ECDHE_RSA_ AES_128_CBC_SHA256
- TLS_ECDHE_RSA_ AES_256_CBC_SHA384
- TLS_ECDHE_RSA_ AES_128_GCM_SHA256
- TLS_ECDHE_RSA_ AES_256_GCM_SHA384
- TLS_ECDHE_ECDSA_ AES_128_CBC_SHA256
- TLS_ECDHE_ECDSA_ AES_256_CBC_SHA384
- TLS_ECDHE_ECDSA_ AES_128_GCM_SHA256
- TLS_ECDHE_ECDSA_ AES_256_GCM_SHA384

For cipher suites using GCM, the IV is generated per RFC 5288. The module supports GCM cipher suites compatible with SP 800-52.

5 Ports and Interfaces

The module ports and interfaces are described in the below table.

Table 8 – Marvell HSM Ports and Interfaces

Physical Ports/Interfaces	Pins Used	FIPS 140-2 Designation	Name and Description
USB Interface	USB Interface USB0_DP, USB0_DM	Power No functionality in FIPS mode	USB Interface Not used in FIPS mode
Serial Interface	3 Pin serial interface - GND, Tx, Rx	N/A No functionality in FIPS mode	Disabled at the hardware level during the firmware load process.
PCIe Interface	PCIE x8 Interface Lane 0 Transmit Side B (14, 15) Receive Side A (16, 17) Lane 1 Transmit Side B (19, 20) Receive Side A (21, 22) Lane 2 Transmit Side B (23, 24) Receive Side A (25, 26) Lane 3 Transmit Side B (27, 28) Receive Side A (29, 30) Lane 4 Transmit Side B (33, 34) Receive Side A (35, 36) Lane 5 Transmit Side B (37, 38) Receive Side A (39, 40) Lane 6 Transmit Side B (41, 42) Receive Side A (43, 44) Lane 7 Transmit Side B (45, 46) Receive Side A (47, 48)	Data Input Control Input Data Output Status Output Power	PCIe Interface - Primary interface to communicate with the module - Provides APIs for the software on the host to communicate with the module
LED	LED interface (7 LEDs, 13 pins)	Status output	Visual status indicator
Tamper PIN	Tamper pin GPIO	Control Input	Tamper pin is used to zeroize the card by zeroizing the master key stored in EEPROM
Power Connector	6 PIN power connector	Power In	External power connector.

6 Identification and Authentication Policy

6.1 Assumption of Roles

The Cryptographic Hardware Security Module enforces identity-based authentication. A role is explicitly selected at authentication; the MCO role is associated with the Master Partition and the PCO and PCU roles are associated with user partitions. The module allows one identity per role.

6.1.1 Manufacturer Role

During the manufacturing stage, each HSM goes through the following process:

- An RSA key pair called the HSM FIPS Master Authentication Key (FMAK) is generated on HSM. CSR is requested out of HSM and signed by the Manufacturer Authentication Root Certificate (MARC). The generated certificate is called the HSM FIPS Master Authentication Certificate (FMAC).
- A 256-bit MKBK encrypted with the FMAK public key is loaded into the HSM.
- Program Performance settings and Appliance Compatibility mode
- Program Serial Number and Max Operating Temperature

The same above steps are followed by the manufacturer once the HSM is moved to manufacturer reset after manufacturer zeroize.

6.1.2 Master Partition Roles

Master partition supports only Cryptographic Officer role, referred to as the Master Crypto Officer (MCO). The Username and password are encrypted with an AES 256 bit key.

6.1.3 Non-Master Partition Roles

Each Non-Master Partition supports two distinct operator roles, Partition Crypto User (PCU) and Partition Crypto Officer (PCO). The module enforces the separation of roles using identity-based authentication. Re-authentication is required to change roles.
Concurrent operators are allowed; however, only one operator is allowed per login session.
The Username is used as the identification for identity-based authentication. The username and password encrypted with an AES 256-bit key is passed during the Login service.
Each non-master partition will have one PCO and one PCU.

6.1.4 Appliance User

Authenticated using a username and password which is encrypted with an AES 256-bit key on entry. For audit logs and offloading Appliance secure channel crypto operations.

6.2 Strength of Authentication

Table 9 – Roles and Required Identification and Authentication

Role	Description	Authentication Type	Authentication Data
Manufacturer	This role sets the identity, serial number, performance settings and max operating temperature	Manufacturer License certificate based authentication	RSA 2048-bit signature on the provided data.
MCO	This role has access to administrative services offered by the module or HSM	Identity-based operator authentication	Case In-Sensitive Username and 7 to 32 character encrypted password.
PCO	This role has access to administrative services of the partition	Identity-based operator authentication	Case In-Sensitive Username and 7 to 32 character encrypted password.
PCU	This role has access to all crypto services offered by the partition	Identity-based operator authentication	Case In-Sensitive Username and 7 to 32 character encrypted password.
Appliance User	This role has access to partition audit logs and Appliance secure channel key.	Identity-based operator authentication	Case In-Sensitive Username and 7 to 32 character encrypted password or RSA 2048 bit signature on the provided data.

Table 10 – Strength of Authentication Mechanism

Authentication Mechanism	Strength of Mechanism
Authentication using password based scheme*	This mode provides a false acceptance rate of 1/78,364,164,096 less than 1/1,000,000), determined by the password. Password is minimum 7 characters, alpha-numeric so it is (26+10)^7 To exceed 1 in 100,000 probability of a successful random attempt during a 1-minute period, 7350919 (122515 per second) attempts would have to be executed. The module limits the number of Login tries to a user configured value "login_fail_count" during module initialization. This configuration value cannot exceed 20. If the user exceeds the configured value for maximum consecutive failed login attempts, then the corresponding user is blocked from login service. A PCO can reset passwords and unblock PCU of his own partition.
Authentication using RSA Signatures	Authentication is performed using SHA-256 based RSA 2048-bit PKCS#1-v1.5 signatures (provides 112 bits of strength). Corresponding public key is part of FW image. The probability that a random attempt will succeed, or a false acceptance will occur is approximately 1/2^112.The fastest the module can process signature verifications is 4,000 per second. Based on this maximum rate, the probability that a random attempt will succeed in a one-minute period is approximately 4,000/2^112.

*Note: The Module supports dual factor authentication where the first factor is a user name and password as described above and the second factor is a digital signature.

6.3 Roles, Services, and CSP Access

G = Generate: The module generates the CSP.
R = Read: The module reads the CSP out of the module.
W = Write: The module writes the CSP. The write access is typically performed after a CSP is imported into the module, or the module generates a CSP, or the module overwrites an existing CSP.
Z = Zeroize: The module zeroizes the CSP.
E = Execute: The module executes or uses the CSP.

Table 11 – Roles, Services and CSPs

MCO	PCO	PCU	Manufacturer	Appliance User	Unauthenticated	Service	Description	Commands	Cryptographic Keys/CSPs
X	X	X	X	X	X	HSM Zeroize	Zeroize: All non-Mfr specific keys/data	CN_ZEROIZE	G: N/A E: N/A R: N/A W: N/A Z: Partial
X	X	X	X	X	X	Partition Zeroize	Zeroize: All non Mfr specific keys/data of partition	CN_ZEROIZE	G: N/A E: N/A R: N/A W: N/A Z: Partial
X						Vendor/ Manufacture Zeroize HSM	Zeroize: all data	CN_VENDOR_ ZEROIZE	G: N/A E: N/A R: N/A W: N/A Z: All
X	X	X	X	X	X	Session Management	Management services for open, status of sessions.	CN_APP_INITIALIZE CN_APP_FINALIZE CN_OPEN_SESSION CN_CLOSE_SESSION CN_GET_SESSION_ NFO	G: N/A E: N/A R: N/A W: N/A Z: N/A
X	X	X	X	X	X	Session Management - Close	Management services for closing all sessions.	CN_CLOSE_ALL_ SESSIONS	G: N/A E: N/A R: N/A W: N/A Z: N/A

MCO	PCO	PCU	Manufacturer	Appliance User	Unauthenticated	Service	Description	Commands	Cryptographic Keys/CSPs
X	X					Partition Application Session Close (All)	Close sessions of all Applications tied to a Partition	CN_CLOSE_PARTITION_SESSIONS	G: N/A E: N/A R: N/A W: N/A Z: N/A
X	X	X	X	X	X	Basic HSM Info	Obtain basic information of the HSM.	CN_TOKEN_INFO CN_PARTITION_INFO CN_GET_HSM_LABEL CN_ALL_PARTITION_INFO CN_GET_HSM_DIAG_INFO	G: N/A E: N/A R: N/A W: N/A Z: N/A
X	X	X				Read Firmware Version String	Obtain firmware version	CN_GET_VERSION	G: N/A E: N/A R: N/A W: N/A Z: N/A
X	X	X	X	X	X	Login to a Session	Allows login to a session. Public key is used to verify user signatures, optionally in 2-factor authentication.	CN_LOGIN	G: N/A E: PswdEncKey R: Password and Two-Factor Authentication Public Key W: N/A Z: N/A
X	X	X		X		Logout of a Session	Allows logout of a session	CN_LOGOUT	G: N/A E: N/A R: N/A W: N/A Z: N/A
X	X	X		X		Change User Password	Requires user to be logged in. Updates Passwords and Public key for 2-factor authentication	CN_CHANGE_PSWD	G: N/A E: PswdEncKey R: N/A W: new password, new public key Z: Old password
X			X			Manufacturer Settings	Manufacturer Controlled Settings run by manufacturer for the first time and MCO can do it later.	CN_MASTER_CONFIG CN_CERT_AUTH_GET_CERT_REQ CN_CERT_AUTH_STORE_CERT CN_STORE_VENDOR_PRE_SHARED_KEY	G: FMAK, MFDEK E: Manufacturer License Validation Key R: CSR of FMAK W: MARC, FMAC, MFKBK Z: N/A

MCO	PCO	PCU	Manufacturer	Appliance User	Unauthenticated	Service	Description	Commands	Cryptographic Keys/CSPs
X						Initialize HSM	Commands and services to initialize the module.	CN_INIT_TOKEN CN_GEN_PSWD_ENC_KEY CN_CREATE_CO CN_INIT_DONE CN_CERT_AUTH_STORE_CERT CN_CERT_AUTH_GET_CERT_REQ CN_CERT_AUTH_STORE_CERT CN_STORE_USER_PRE_SHARED_KEY	G: HSM PswdEncKey RSA key pair, PswdEncKey, E: PswdEncKey, MFDEK R: CSR for FMAK W: Host PswdEncKey Public Key, AOAC, Password, Two-Factor Authentication Public key, AOTAC Z: N/A
				X		Secure Boot	Commands to identify the hosts are of Marvell	CN_CERT_AUTH_GET_CERT CN_CERT_AUTH_RECV_PEER_CERT CN_CERT_AUTH_SECURE_BOOT	G: N/A E: MARC to validate HOST_ID Certificate, HOST_ID Certificate to validate signature on challenge R: FMAC W: N/A Z: N/A
X						Firmware Update	Updates adapter with Marvell signed firmware images. Adapter has to be rebooted to use the new firmware.	CN_FW_UPDATE_BEGIN CN_FW_UPDATE CN_FW_UPDATE END	G: N/A E: Manufacturer Firmware Validation Key R: N/A W: Manufacturer Firmware Validation Key, Manufacturer License Validation Key Z: N/A
X						Other MCO Operations	Misc. MCO Operations	CN_SLAVE_CONFIG CN_INVOKE_FIPS	G: N/A E: N/A R: N/A W: N/A Z: N/A
X						Partition Management	Commands and services to manage partitions	CN_CREATE_PARTITION CN_DELETE_PARTITION CN_RESIZE_PARTITION CN_GET_PARTITION_COUNT CN_ALL_PARTITION_INFO	G: PAK key pair, PMEK E: FMAK R: N/A W: PAC Z: All partition keys

MCO	PCO	PCU	Manufacturer	Appliance User	Unauthenticated	Service	Description	Commands	Cryptographic Keys/CSPs
X						MCO Backup and Restore	Allows MCO to take back up using KBK derived from pre-loaded MKBK, OKBK. MCO uses find key in to get the key handles in a partition	CN_BACKUP_BEGIN CN_BACKUP_CONFIG CN_BACKUP_USERS CN_BACKUP_KEY CN_BACKUP_END CN_RESTORE_BEGIN CN_RESTORE_CONFIG CN_RESTORE_USERS CN_RESTORE_KEY CN_RESTORE_END	G: KBK, User passwords and Two-Factor Authentication Public Keys, All user keys E: MFKBK, OKBK, KBK R: POTAC, All keys NIST AES wrapped with KBK W: All keys NIST AES wrapped with KBK, new POTAC verify the owner ship Z: N/A
	X					PCO Backup and Restore	PCO uses find key in to get the key handles in a partition	CN_BACKUP_BEGIN CN_CREATE_OBJECT CN_WRAP_KBK (Modes: KBK_WRAP_WITH_KEK, KBK_WRAP_WITH_CERT_AUTH_DERIVED_KEY, KBK_WRAP_WITH_RSA) CN_BACKUP_CONFIG CN_BACKUP_USERS CN_BACKUP_KEY CN_BACKUP_END CN_RESTORE_BEGIN CN_GENERATE_KEY_PAIR CN_UNWRAP_KBK (Modes: KBK_WRAP_WITH_KEK, KBK_WRAP_WITH_CERT_AUTH_DERIVED_KEY, KBK_WRAP_WITH_RSA) CN_RESTORE_CONFIG CN_RESTORE_USERS CN_RESTORE_KEY CN_RESTORE_END	G: User passwords and Two-Factor Authentication Public Keys, All user keys, KBK Wrapping RSA key pair, POKBK E: KLK or KBK Wrap RSA public key or CertAuthTokenKey, Partition KBK, R: wrapped Partition KBK, W: KBK wrap public key, All keys NIST AES wrapped with KBK Z: N/A
X						MCO Partition Data Management	Commands to manage Unclassified data storage mainly used to maintain network IP addresses	CN_PARTN_STORAGE_UPDATE CN_PARTN_STORAGE_GET CN_PARTN_STORAGE_DELETE	G: N/A E: N/A R: N/A W: N/A Z: N/A

MCO	PCO	PCU	Manufacturer	Appliance User	Unauthenticated	Service	Description	Commands	Cryptographic Keys/CSPs
	X					Partition Initialization	Commands to initialize the partition and claim ownership of the partition	CN_INIT_TOKEN CN_GEN_PSWD_ ENC_KEY CN_CREATE_CO CN_INIT_DONE CN_CERT_AUTH_ GET_CERT_REQ CN_CERT_AUTH_ STORE_CERT CN_STORE_USER_ PRE_SHARED_ KEY	G: Partition PswdEncKey key pair, PswdEncKey, E: PswdEncKey, FMAK R: CSR for PAK W: Host PswdEncKey Public Key, Password, Two-Factor Authentication Public key, POAC, POTAC, POKBK Z: N/A
	X					PCO User Management	Commands to manage users in the partition	CN_CREATE_USER CN_DELETE_USER CN_LIST_USERS CN_GET_LOGIN_ FAILURE_CNT	G: N/A E: PswdEncKey to decrypt and store, PMEK to encrypt the password and store it in database R: N/A W: password and new Public key Z: all session keys
X	X					SecureAuth based on Certificates	Commands used for mutual authentication and key agreement between two partitions/entities of same Partition owner on Cavium HSM.	CN_CERT_AUTH_ GET_CERT CN_CERT_AUTH_ GET_SOURCE_ RANDOM CN_CERT_AUTH_ VALIDATE_PEER_ CERTS CN_CERT_AUTH_ GET_CERT CN_CERT_AUTH_ VALIDATE_PEER_ CERTS CN_CERT_AUTH SOURCE_KEY_ EXCHANGE	G: N/A E: POTAC to verify peer POAC, MARC to verify peer PAC and FMAC, peer PAC to verify peer signature, local PAK to sign responder's challenge, local PAK to sign initiator's challenge R: FMAC, PAC, POAC, W: Peers FMAC, PAC, POAC, Z: N/A

MCO	PCO	PCU	Manufacturer	Appliance User	Unauthenticated	Service	Description	Commands	Cryptographic Keys/CSPs
	X					Cloning Protocol	Cloning: Clone Masking of a Partition to a different Partition of the same owner.	CN_CLONE_SOURCE_INIT CN_CLONE_SOURCE_STAGE1 CN_CLONE_TARGET_INIT CN_CLONE_TARGET_STAGE1	G: Partition's Masking Key, KAS key pair, Z and KAS keying material, Partition's Cloning Private Key E: KAS keying material for masking key encryption and mac tag generation and peer mac tag verification, KAS keying material for presumed data encryption and mac tag generation, KAS keying material to decrypt the masking key, validate MAC tag. R: Partition Cloning/KLK Initiator Public Key, Partition Cloning/KLK Responder Public Key W: Partition Cloning/KLK Initiator Public Key, Partition Cloning/KLK Responder Public Key Z: Z and KAS keying material
		X				Key Transportation	A SP 800-56 A/B protocol to generate a shared KLK on host and Partition.	CN_GEN_KEY_ENC_KEY	G: Partition KLK RSA/ECC key pair, KLK E: N/A R: N/A W: Host RSA/ECC KLK Public Key Z: N/A

MCO	PCO	PCU	Manufacturer	Appliance User	Unauthenticated	Service	Description	Commands	Cryptographic Keys/CSPs
		X				PCU Key Management		CN_EXTRACT_MASKED_OBJECT CN_INSERT_MASKED_OBJECT CN_DESTROY_OBJECT CN_GET_ATTRIBUTE_VALUE CN_GET_ATTRIBUTE_SIZE CN_MODIFY_OBJECT CN_FIND_OBJECTS CN_FIND_OBJECTS_FROM_INDEX CN_GENERATE_KEY CN_GENERATE_KEY_PAIR CN_GENERATE_PBE_KEY CN_EXPORT_PUB_KEY	G: General Purpose User CSPs, General Purpose User Public Keys E: Masking Key, KLK or user provided wrapping Key, PEK specified user key, all user keys, R: General Purpose User CSPs, General Purpose User Public Keys W: Imported keys Z: General Purpose User CSPs, General Purpose User Public
X	X	X		X		Find Key handles	Users can find key handles based on search criteria like key type or label. MCO/PCO use it as part of backup service	CN_FIND_OBJECTS CN_FIND_OBJECTS_FROM_INDEX	G: N/A E: N/A R: All user keys W: N/A Z: N/A
				X		PCU Key Management – Special	Unwrap only RSA Key	CN_UNWRAP_KEY CN_FIND_OBJECT CN_DELETE_OBJECT	G: N/A E: KLK R: Asymmetric Private Key (RSA only) W: Asymmetric Private Key (RSA only) Z: Asymmetric Private Key (RSA only)
		X		X		PCU Crypto Offload	CN_ME_PKCS and CN_ME_PKCS_LARGE are RSA 2K and 3K operations. Appliance user is allowed to use the imported RSA key.	CN_SIGN CN_VERIFY CN_ECC_DH CN_NIST_AES_WRAP CN_ALLOC_SSL_CTX CN_FREE_SSL_CTX CN_GEN_PMK CN_FIPS_RAND CN_ME_PKCS_LARGE CN_ME_PKCS CN_FECC CN_HASH CN_HMAC CN_ENCRYPT_DECRYPT	G: N/A E: specified user key R: N/A W: N/A Z: N/A

MCO	PCO	PCU	Manufacturer	Appliance User	Unauthenticated	Service	Description	Commands	Cryptographic Keys/CSPs
	X			X		Audit Logs – PCO / Appliance		CN_PARTN_GET_ AUDIT_DETAILS CN_PARTN_GET_ AUDIT_LOGS CN_PARTN_GET_ AUDIT_SIGN	G: N/A E: PAK, FMAK R: N/A W: N/A Z: N/A
X						Audit Logs – MCO		CN_ADMIN_GET_ PARTN_AUDIT_ DETAILS CN_ADMIN_GET_ PARTN_AUDIT_ LOGS CN_ADMIN_GET_ PARTN_AUDIT_ SIGN	G: N/A E: FMAK R: N/A W: N/A Z: N/A
		X				SSL Protocol Packet Processing	These API can understand the SSL/TLS protocol semantics and optimized to do multiple sequential crypto operations on the given input data. For example: Encrypt/decrypt record will do HMAC comparison in addition to the symmetric crypto operation.	MAJOR_OP_RSASERVER _LARGE MAJOR_OP_RSASERVER MAJOR_OP_HANDSHAK E MAJOR_OP_OTHER MAJOR_OP_FINISHED MAJOR_OP_RESUME MAJOR_OP_ENCRYPT_D ECRYPT_RECORD MAJOR_OP_ECDH	G: N/A E: TLS Session Symmetric Key Set and TLS Session HMAC key part of SSL Context R: N/A W: N/A Z: N/A

7 Keys and Certificates

7.1 Definition of Critical Security Parameters (CSPs)

The Manufacturer FIPS Data Encryption Key (MFDEK) and HSM Master Partition Master Encryption Key are stored in plaintext form in the EEPROM. The Partition Master Encryption Key (PMEK) is stored encrypted under the HSM Master Partition Master Encryption Key. All other keys and CSPs stored in the persistent memory are encrypted by the MFDEK, HSM Master Partition Master Encryption Key, or PMEK.

Table 12 – Private Keys and CSPs

Name	Description and Usage
HSM CSPs	
DRBG Entropy	The entropy material for the FIPS Approved DRBG. Instantiates the DRBG with 256-bits of security strength.
CTR_DRBG Internal State	The internal state for the FIPS Approved DRBG.
Manufacturer FIPS Data Encryption Key (MFDEK)	AES 256-bit key used to encrypt manufacturer keys stored in persistent storage of the HSM.
HSM Master Partition Master Encryption Key	AES 256-bit key used to encrypt Master Partition CSPs and authentication data stored in persistent storage of the HSM.
Partition Master Encryption Key (PMEK)	AES 256-bit key used to encrypt partition CSPs and authentication data stored in persistent storage of the HSM.
HSM FIPS Master Authentication Key (FMAK)	A unique 2048-bit RSA private key. Used to identify the HSM when in the FIPS operating mode
Partition Authentication Key (PAK)	A unique 2048-bit RSA private key used to identify the HSM Partition
Authentication CSP	
HSM PswdEncKey RSA Private Key	2048-bit RSA Private Key, used in SP 800-56B KAS to generate PswdEncKey
PswdEncKey	AES-256 key, for encrypting User passwords during user creation and authentication
Login Passwords	String of 7 to 32 alphanumeric characters
Key Loading CSPs	
Partition's KeyLoading Private Key	ECC 512-bit or RSA 2048-bit key used in SP 800-56A C (0,2, ECC DH) or SP 800-56B KAS2 to agree on Z during key loading
Partition's KeyLoading Shared Secret (Z)	Shared secret Z for SP 800-56A C (0,2, ECC DH) or SP 800-56B KAS2
Partition's Key Loading Key (KLK)	A 256-bit AES key derived from Z, used to decrypt the imported CSPs
Backup and Restore Keys	
Manufacturer FIPS Key Backup Key (MFKBK)	AES 256-bit key used to derive KBK
HSM Owner KBK (OKBK)	AES 256-bit key used to derive KBK
Partition Owner KBK (POKBK)	AES 256-bit key used to derive KBK
HSM Key Backup Key (KBK)	Key used to encrypt/decrypt the Backup Session Key
Backup Session Key	Key used to backup and restore partition data
Cloning Keys	
Partition's Cloning Private Key	ECC 512-bit or RSA 2048-bit Static Private Key used in SP 800-56A C(0,2,ECC DH) or SP 800 -56B KAS2 -bilateral -confirmation key agreement to generate shared secret Z. At HSM Partition level, used to establish secure channel for cloning process (to export Masking Key).

Name	Description and Usage
Partition's Cloning Shared Secret (Z)	Shared secret Z for SP 800-56A C (0, 2, ECC DH) or SP 800-56B KAS2 - bilateral -confirmation scheme.
Partition's Cloning Session Key	AES 256 key for encryption and decryption of Masking Key.
Partition's Cloning Session MAC Key	HMAC SHA256 key used for key confirmation during SP 800-56A key agreement
Partition's Masking Key	AES-256 key, for key wrapping. Used to import/export CSPs and masked objects.
General Purpose User CSPs	
Asymmetric Private Keys	RSA/DSA/ECDSA/ECDH general purpose keys
Asymmetric Private Session Keys	RSA/DSA/ECDSA/ECDH general purpose session keys
Symmetric Keys	Triple-DES or AES general purpose keys
Symmetric Session Keys	Triple-DES or AES general purpose session keys
HMAC Keys	HMAC general purpose keys (minimum key size of 160 bits)
HMAC Session Keys	HMAC session general purpose keys (minimum key size of 160 bits)
TLS Session Symmetric Key Set	AES 128, 192, 256 or Triple-DES keys used for encrypting TLS sessions
TLS Session HMAC key	HMAC key used in SSL session (minimum key size of 160 bits)
EAP-FAST-PAC	EAP-FAST authentication Info

Non-Deterministic Random Number Generation Specification

Entropy Sources	Minimum Number of Bits of Entropy	Details
Octeon HW RBG	Entropy source provides the DRBG with sufficient entropy to claim a security strength of 256 bits.	The Octeon II HW unit generates random bits from the 8-free running oscillators from a total of 128-free running oscillators. And the generated random bits are run through software/firmware health tests (APT and RCT). The entropy source supplies the DRBG with 3161 bytes for the entropy input and another 3161 bytes for the nonce. With a minimum entropy assessment of 0.081 bits per byte, this is sufficient to claim a DRBG security strength of 256

7.2 Definition of Public Keys

The module contains the following public keys:

Table 13 – Public Keys

Name	Description and Usage
HSM Keys	
Manufacturer Firmware Validation Key	RSA 2048-bit public key used to authenticate SW images loaded into the module. The SW image is signed by the manufacturer using an RSA private key and the signature is verified before upgrading to the new image using the public key.
Manufacturer License Validation Key	RSA 2048-bit public key used to authenticate the manufacturer role
Manufacturer Authentication Root Cert. (MARC)	RSA 2048-bit public key certificate, used to issue FMAC certificates
HSM FIPS Master Authentication Certificate (FMAC)	RSA 2048-bit public key certificate of FMAK. Used to identify the HSM FIPS operating mode.
SecureBootAuth Public Key	RSA 2048-bit public key used to verify authenticity of the host system
Administrative Keys	
HSM/Adapter Owner Trust Anchor Certificate (AOTAC)	RSA 2048-bit public key certificate used as trust anchor of MCO
HSM/Adapter Owner Authentication Certificate (AOAC)	RSA 2048-bit public key certificate of FMAK. Used to identify the HSM owner.
Partition Authentication Certificate (PAC)	RSA 2048-bit public key certificate of PAK. Used to identify the Partition.
Partition Owner Trust Anchor Certificate (POTAC)	RSA 2048-bit public key certificate used as trust anchor of PCO.
Partition Owner Authentication Certificate (POAC)	RSA 2048-bit public key certificate of PAK. Used to identify the Partition owner.
HOST_ID Certificate	RSA 2048-bit public key certificate used to authenticate HSM users trusted by Vendor
Key Backup/Cloning Keys	
Partition Cloning/KLK Initiator Public Key	ECC 512-bit static public key used in SP 800-56A C (0, 2, ECC DH) key agreement or RSA 2048-bit static public key used in SP 800-56B KAS2 -bilateral -confirmation key agreement to generate shared secret Z.
Partition Cloning/KLK Responder Public Key	ECC 512-bit static public key used in SP 800-56A C (0, 2, ECC DH) key agreement or RSA 2048-bit static public key used in SP 800-56B KAS2 -bilateral -confirmation key agreement to generate shared secret Z.
Partition Cloning ECC Domain Parameter Set	Set EE per SP 800-56A Table 2
Authentication Keys	
Partition PswdEncKey Public Key	RSA 2048-bit public key generated by the partition to be used in SP 800-56B key agreement to generate PswdEncKey.
Host PswdEncKey Public Key	RSA 2048-bit public key loaded by the host to be used SP 800-56B key agreement to generate PswdEncKey.
Two-Factor Authentication Public Key	RSA 2048-bit public key used to verify signature on encrypted passwords during user creation and login
General Purpose Keys	
User Public Keys	RSA/DSA/ECDSA/ECDH public keys
User Public Session Keys	RSA/DSA/ECDSA/ECDH public session keys

7.3 Definition of Session Keys

The cryptographic module supports the generation/import/export of user keys which are bound to a session and are termed as session keys. Following points apply to the session keys:

- Session keys are stored in RAM and are lost across reboots.
- Session key access is restricted to an application in which it is created.
- Every session in an application will have access to the keys created by every other session in the same application.
- When a session is closed, the session keys created by that session get destroyed.

8 Operational Environment

The module implements a limited operational environment. FIPS 140-2 Area 6 Operational Environment requirements do not apply to the module in this validation.

9 Security Rules

This section documents the security rules enforced by the cryptographic module to implement the security requirements of this FIPS 140-2 Level-3 module.

1. The cryptographic module clears previous authentications on power cycle.
2. When the module has not been placed in a valid role, the operator shall not have access to any cryptographic services.
3. The cryptographic module shall perform the following power up, continuous and conditional self-tests:

   A. Power-Up Tests
   - AES (CBC and ECB) Encrypt & Decrypt KATs (NitroxIII, Cert. #2034)
   - AES (GCM) Encrypt & Decrypt KATs (NitroxIII, Cert. #2035)
   - AES (ECB) Encrypt & Decrypt KATs (NitroxIII, Cert. #2033)
   - HMAC SHA-1, 224, 256, 384, 512b KATs (NitroxIII, Cert. #1233)
   - TLS 1.0/1.1/1.2 KDF KAT (NitroxIII, CVL Cert. #167)
   - SHA-1, 224, 256, 384, 512 KATs (NitroxIII, Cert. #1780)
   - Triple-DES (TCBC) Encrypt & Decrypt KATs (NitroxIII, Cert. #1311)
   - AES (ECB) Encrypt & Decrypt KATs for DRBG, Key wrap (Firmware, Cert. #3205)
   - AES Key Wrap Encrypt & Decrypt KATs (Firmware, Cert. #3206)
   - SP 800-90A CTR_DRBG KAT (Firmware, Cert. #680)
   - DSA Sig Gen, Sig Ver, PQG Gen, PQG Ver, and Key Gen KATs (Firmware, Cert. #916)
   - ECDSA Sig Gen and Sig Ver KATs (Firmware, Cert. #589)
   - HMAC-SHA-1, 224, 256, 384, 512 KATs (Firmware, Cert. #2019)
   - KAS (Shared Secret Calculation and KDF) KAT (Cert. #A1934)
   - RSA Sig Gen, Sig Ver KATs (Firmware, Cert. #1634)
   - SHA-1, 224, 256, 384, 512 KATs (Firmware, Cert. #2652)
   - RSA Encrypt & Decrypt KAT (Firmware, Cert. #A1935 and #A1936)
   - ECC CDH KAT (NitroxIII, CVL Cert. #563)
   - RSA Encrypt & Decrypt KAT (NitroxIII, Cert. #A1937)
   - OCTEON SP800-108 KBKDF KAT (Firmware, Cert #65)
   - Firmware integrity test (CRC-16)

   B. Conditional Self-Tests
   - ECDSA Pairwise Consistency Test
   - RSA Pairwise Consistency Test
   - DSA Pairwise Consistency Test
   - SP 800-90A CTR_DRBG Continuous number test
   - SP 800-56Ar3, Section 5.6.2 Assurances per IG D.8
   - SP 800-56Br2, Section 6.4 Assurances per IG D.8

- HW RNG Continuous Number Test
- Firmware load test (RSA Signature Verification)
- DRBG, SP800-90A health tests (Instantiate, Generate and Reseed).
- SP800-90B entropy health tests (RCT, APT).

4. Critical Functions Tests: The module runs the following Critical Functions Tests which are required to ensure the correct functioning of the device.
    a. Power On Memory Test
    b. EEPROM Test
    c. NOR Flash Test
    d. Nitrox Chips Tests
5. The operator shall be capable of commanding the module to perform the power up self-test by cycling power or resetting the module.
6. Power up self-tests do not require any operator action.
7. Data output shall be inhibited during self-tests, zeroization, and error states.
8. Status information does not contain CSPs or sensitive data that if misused could lead to a compromise of the module.
9. There are no restrictions on which keys or CSPs are zeroized by the zeroization service.
10. The module does not support a maintenance interface or role.
11. The module does not support bypass capabilities.
12. The module does not support manual key entry.
13. The module has no CSP feedback to operators.
14. The module does not enter or output plaintext CSPs
15. The module does not output intermediate key values.
16. The module shall be configured for FIPS operation by following the first-time initialization procedure described in User Manual and C-API Specification (CN16xx-NFBE-API-0.9).

10 Physical Security Policy

10.1 Physical Security Mechanisms

The module's cryptographic boundary is defined to be the outer perimeter of the hard epoxy enclosure containing the hardware and firmware components. The module is opaque and completely conceals the internal components of the cryptographic module. The epoxy enclosure of the module prevents physical access to any of the internal components without having to destroy the module. There are no operator required actions.
Note: The module's hardness testing was only performed at ambient temperature (23°C); no assurance is provided for Level 3 hardness conformance at any other temperature.

11 Mitigation of Other Attacks Policy

No mitigation of other attacks is implemented by the module.

12 References

1. NIST AES Key Wrap Specification, SP 800-38F, December 2012
2. NIST Special Publication 800-56A Rev. 3, April 2018.

3. NIST Special Publication 800-56B Rev. 2, March 2019.
4. NIST Special Publication 800-57 Part-5, May 2020.
5. FIPS PUB 186-4, Digital Signature Standard (DSS), July 2013
6. FIPS PUB 140-2, FIPS Publication 140-2 Security Requirements for Cryptographic Modules
7. Implementation Guidance for FIPS PUB 140-2 and the Cryptographic Module Validation Program
8. NIST Special Publication 800-131A Rev. 2, March 2019.

13 Definitions and Acronyms

MCO – Master Crypto Officer

PCO – Partition Crypto Officer

PCU – Partition Crypto User

HSM – Hardware Security Module

KBK – Key Backup Key

KLK – Key Loading Key

KAT – Known Answer Test

KAS – Key Agreement Scheme

14 Appendix A: Supported ECC curves for Sig-Verify

Curves over prime number fields: P-192, P-224, P-256, P384, P-521.

Koblitz curves over 2^m fields: K-163, K-233, K-283, K-409, K-571.

Curves over 2^m fields: B-163, B-233, B-283, B-409, B-571.

15 Appendix B: Supported ECC curves for Key-Gen and Sig-Gen

Curves over prime number fields: P-224, P-256, P384, P-521.

Koblitz curves over 2^m fields: K-233, K-283, K-409, K-571.

Curves over 2^m fields: B-233, B-283, B-409, B-571.